NUI Galway
OÉ Gaillimh

Semester 2 Examinations 2013/ 2014

Exam Code(s)	4BCT1
Exam(s)	BSc in Computer Science and Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. M. Madden *Dr. C. Mulvihill

Instructions: Answer any 4 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	2
Discipline(s)	Information Technology
Course Co-ordinator(s)	

Requirements:

MCQ	Release to Library: Yes [X] No [ ]
Handout	None
Statistical/ Log Tables	None
Cambridge Tables	None
Graph Paper	None
Log Graph Paper	None
Other Materials	None
Graphic material in colour	Yes [ ] No [X]

PTO

1

(a) What is meant by the terms ‘stream cipher’ and ‘block cipher’? (4 marks)

(b) 'Block ciphers are found with many modes of operation such as Cipher Feedback Mode, Cipher Block Chain, and Counter Mode.’ Give an account of Counter Mode, giving any one advantage and any one disadvantage that you see with this mode of operation (6 marks)

(c) You have been asked to review a student project proposal for a stream cipher. The proposal reads: ‘A plaintext message is enciphered with our own stream cipher. There is a keystream that performs an XOR with each plaintext bit. The plaintext is recovered by performing a further XOR on the ciphertext with the same keystream. The keystream is in fact a repeating short key (currently a byte); our group does not see any need whatsoever at this time for a so-called keystream generator.’ Advise the group on the state of their proposal. (10 marks)

2

(a) ‘Public-key systems often depend on so-called trapdoor one-way functions’. Explain what is meant by the term ‘trapdoor one-way function’ (4 marks)

(b) In the context of public-key cryptography, explain what is meant by the terms ‘public key’, ‘private key’ and ‘certification authority’(6 marks)

(c) Alice is working on an assignment for her tutor Emma. Alice decides to consult Bob, who is in her class. Alice signs her assignment work with her private signature key. She then encrypts all of this with Bob's public encryption key. She sends the resulting message to Bob for comments. Bob decrypts the message and reads the assignment work. He finds an error but instead of informing Alice, he encrypts the signed assignment with Emma’s public key and sends it on. Emma believes that the assignment work is from Alice and Alice receives a low grade. Advise Alice on how to deal with this scenario (10 marks)

3

(a) Distinguish between a hash function and a MAC (message authentication code) (5 marks)

(b) 'To achieve data origin authentication for a digital signature scheme with a symmetric MAC key, a trusted third party (ttp) or arbitrator should be employed'. By considering two parties communicating via a ttp, illustrate the operation of such a scheme. (7 marks)

(c) ‘An RSA digital signature with appendix involves the use of a hash function’. Give a brief account of how signing and verification works with such a scheme. (8 marks)

PTO

4

(a) 'A dynamic password scheme often involves a challenge and a response, and the use of a so-called token that implements a password function and an associated key.' Briefly outline the operation of such a scheme (6 marks)

(b) Freshness in a communication is sometimes provided by a clock, perhaps also by sequence numbers, or sometimes through nonce mechanisms. Mention any one special requirement for each of these three schemes. (6 marks)

(c) Briefly outline what is meant by 'zero-knowledge entity authentication', using any analogy of your choice to illustrate your answer. (8 marks)

5

(a) Give your understanding of the terms confidentiality, integrity, and availability in the context of computer security. (6 marks)

(b) What type of access environment might be expected to enforce 'no write up' and 'no read down' modes between subjects and objects? Explain what is meant by 'no read down' and 'no write up' in the course of your answer. (6 marks)

(c) Your organisation is considering installing and customising an infrastructure for criminal investigations. Confidentiality of data has been identified as the single most important issue to be addressed. Would access modes such as that in **5 (b)** be the most suitable? If not, what would you suggest? (8 marks)

6

(a) Explain what is meant by the 'Daubert Criteria' and discuss why they are considered relevant in the context of computer forensics. (6 marks)

(b) You are an IT officer for a medium-sized Irish company and have found a steganographic program on a copy of a hard disk that originates from a laptop associated with an office housing several junior employees. Your organisation is heavily involved in confidential IP negotiations at this time, and the security policy in place does not permit such software to be in the possession of such employees. In the light of your understanding of security policies, what response or responses would you consider appropriate? (6 marks)

(c) Give an account of the importance of email headers in network forensics. (8 marks)

7

"Cryptographic protocols are often to be found on the Internet." Discuss this statement with reference to the handshake (8 marks) and record (8 marks) protocols of SSL, explaining the term 'protocol' (4 marks) in the course of your answer. (20 marks in total)